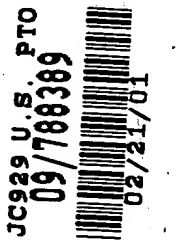
#2 Priority 4/12/01 KPannell

Docket No. 1614.1127/HJS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE



In re Application of:

Mitsuru NAKAJIMA et al.

Group Art Unit:

Serial No.:

Examiner:

Filed: February 21, 2001

For: AUTHENTICATION METHOD, AUTHENTICATION SYSTEM....

SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application(s):

Japanese Patent Application No. 2000-256340
Filed: August 25, 2000

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date, as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: February 21, 2001

By: _____

H. J. Staas
Registration No. 22,010

700 Eleventh Street, N.W., Suite 500
Washington, D.C. 20001
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

日　本　国　特　許　庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年　８月２５日

出願番号
Application Number: 特願２０００－２５６３４０

出願人
Applicant (s): 富士通株式会社

２０００年１２月　１日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２０００－３１０１１８１

【書類名】　特許願

【整理番号】　0050522

【提出日】　平成12年 8月25日

【あて先】　特許庁長官　及川　耕造　殿

【国際特許分類】　G06F 15/20

【発明の名称】　認証処理方法、認証処理システム、決済方法、利用者装置及び認証処理を行うためのプログラムを格納した記憶媒体

【請求項の数】　10

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　中島　充

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　今嶋　佳明

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　半田　高敬

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　門間　仁

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　小高　敏裕

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　藤井　美香子

【特許出願人】

【識別番号】　000005223

【氏名又は名称】　富士通株式会社

【代理人】

【識別番号】　100070150

【住所又は居所】　東京都渋谷区恵比寿４丁目２０番３号　恵比寿ガーデンプレイスタワー３２階

【弁理士】

【氏名又は名称】　伊東　忠彦

【電話番号】　03-5424-2511

【手数料の表示】

【予納台帳番号】　002989

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9704678

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　認証処理方法、認証処理システム、決済方法、利用者装置及び認証処理を行うためのプログラムを格納した記憶媒体

【特許請求の範囲】

【請求項１】　取引を行う利用者間の認証に関する処理を行う認証処理システムにおける認証処理方法において、

前記利用者間で予定した取引に関して第２の利用者に照合キーを通知するステップと、

第２の利用者に通知された照合キーを第２の利用者より第１の利用者が受け取った後に、第１の利用者から通知される前記第２の利用者の照合キーの照合を行うステップとを有することを特徴とする認証処理方法。

【請求項２】　請求項１記載の認証処理方法において、

前記認証処理システムは、照合キーを通知するステップに先だって、利用者の個人認証を行うことを特徴とする認証処理方法。

【請求項３】　請求項１記載の認証処理方法において、

前記取引が予め設定された利用可能金額内であるか否かの判定を行うことを特徴とする認証処理方法。

【請求項４】　請求項１記載の認証処理方法において、

前記取引が予め設定された取引条件に適合するか否かの判定を行うことを特徴とする認証処理方法。

【請求項５】　請求項１記載の認証処理方法において、

前記照合キーを通知するステップは、双方の利用者に異なる照合キーを通知することを特徴とする認証処理方法。

【請求項６】　請求項１記載の認証処理方法において、更に、

前記利用者間で予定した取引に関して第１の利用者に照合キーを通知するステップと、

第１の利用者に通知された照合キーを第１の利用者より第２の利用者が受け取った後に、第２の利用者から通知される前記第１の利用者の照合キーの照合を行うステップとを有することを特徴とする認証処理方法。

【請求項７】　請求項１ないし６いずれか一項記載の認証処理方法における照合結果に基づいて、決済処理を行うことを特徴とする決済方法。

【請求項８】　取引を行う利用者間の認証を行う認証処理システムにおいて、

前記利用者間で予定した取引に関して第２の利用者に照合キーを通知する通知手段と、

第２の利用者に通知された照合キーを第２の利用者より第１の利用者が受け取った後に、第１の利用者から通知される前記第２の利用者の照合キーの照合を行う照合手段とを有することを特徴とする認証処理システム。

【請求項９】　取引を行う利用者間の認証に関する処理を行う利用者装置において、

該取引に関して各利用者に異なる照合キーを通知する認証処理システムに、前記利用者間で予定した取引に関する情報を送信する第１の送信手段と、

前記認証システムからの該取引に関する照合キーを受信する第１の受信手段と、

利用者間で前記照合キーを通知し合った後に、照合キーの照合を行う認証処理システムに、相手から通知された相手側の照合キーを、送信する第２の送信手段と、

前記認証処理システムから照合結果を受信する第２の受信手段とを有することを特徴とする利用者装置。

【請求項１０】　取引を行う利用者間の認証に関する処理を行うためのプログラムを格納した記憶媒体であって、

コンピュータを動作させて、

該取引に関して各利用者に異なる照合キーを通知する認証システムに、前記利用者間で予定した取引に関する情報を送信する第１の送信手段と、

前記認証システムから該取引に関する照合キーを受信する第１の受信手段と、

利用者間で前記照合キーを通知し合った後に、照合キーの照合を行う認証処理システムに、相手から通知された相手側の照合キーを、送信する第２の送信手段と、

前記認証処理システムから照合結果を受信する第２の受信手段とを機能させるためのプログラムを格納したことを特徴とする記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、認証処理方法、認証処理システム、決済方法、利用者装置及び認証処理を行うためのプログラムを格納した記憶媒体に関する。

【０００２】

【従来の技術】

対面販売において、購入者は、現金があれば、現金で決済するが、現金がない場合はクレジットカードで決済を行う。クレジットカードは、サインをするだけで、カード会社の加盟店から一定限度内の買物ができる。

【０００３】

現在、クレジットカードは、現金を持ち歩かなくて済むことから、カード社会と言われる程に、普及している。

【０００４】

また、昨今のインターネットの普及に伴い、インターネットを利用して、オンラインショッピングが行われている。この場合、決済手段として、会員番号、パスワード等を送信して、決済することも行われている。

【０００５】

【発明が解決しようとする課題】

しかしながら、対面販売において、クレジットカードなどにより決済を行う場合、取り扱い加盟店の信憑性やカード番号のスキミングなど、安全性の面から問題が指摘されている。また、加盟店側においても、カード所有者が本人であるか否かの確認を行うことは困難であるという問題がある。

【０００６】

また、オンラインショッピング等で、会員番号、パスワード等を、インターネット上に送信して決済することは、会員番号、パスワード等が傍受されるという危険があり、場合によっては、会員番号、パスワード等が盗まれ、本人に代わっ

て使用されるという問題がある。

【０００７】

本発明は、上記問題に鑑みなされたものであり、テンポラリな情報で認証を可能とし、安全で利便性の高い認証・決済手段を提供することを目的とするものである。

【０００８】

【課題を解決するための手段】

上記課題を解決するために、本件発明は、以下の特徴を有する課題を解決するための手段を採用している。

【０００９】

請求項１に記載された発明は、取引を行う利用者間の認証に関する処理を行う認証処理システムにおける認証処理方法において、前記利用者間で予定した取引に関して第２の利用者（例えば、図１における利用者Ｂ）に照合キーを通知するステップと、第２の利用者に通知された照合キーを第２の利用者より第１の利用者（例えば、図１における利用者Ａ）が受け取った後に、第１の利用者から通知される前記第２の利用者の照合キーの照合を行うステップ（例えば、図４におけるステップ２６）とを有することを特徴とする。

【００１０】

請求項１記載の発明によれば、利用者間で予定した取引に関して第２の利用者に照合キーを通知し、更に、第２の利用者に通知された照合キーを第２の利用者より第１の利用者が受け取った後に、第１の利用者から通知される前記第２の利用者の照合キーの照合を行うことにより、テンポラリな情報で認証が可能となり、安全で利便性の高い認証を行うことができる。

【００１１】

請求項２に記載された発明は、請求項１記載の認証処理方法において、前記認証処理システムは、照合キーを通知するステップに先だって、利用者の個人認証を行う（例えば、図２におけるステップ１１、ステップ１２）ことを特徴とする。

【００１２】

請求項２記載の発明によれば、認証処理システムは、照合キーを通知するステップに先だって、利用者の個人認証を行うことにより、取引当事者は、相手の資格・当事者能力について心配することなく、安心して取引を行うことができる。

【００１３】

請求項３に記載された発明は、請求項１記載の認証処理方法において、前記取引が予め設定された利用可能金額内であるか否かの判定を行うことを特徴とする。

【００１４】

請求項３記載の発明によれば、取引が予め設定された利用可能金額内であるか否かの判定を行うことにより、取引当事者は、金額の心配をすることなく、安心して取引を行うことができる。

【００１５】

請求項４に記載された発明は、請求項１記載の認証処理方法において、前記取引が予め設定された取引条件に適合するか否かの判定を行うことを特徴とする。

【００１６】

請求項４記載の発明によれば、取引が予め設定された取引条件に適合するか否かの判定を行うことにより、取引当事者は、取引条件に関して心配をすることなく、安心して取引を行うことができる。

【００１７】

請求項５に記載された発明は、請求項１記載の認証処理方法において、前記照合キーを通知するステップは、双方の利用者に異なる照合キーを通知する（例えば、図４におけるステップ２１、ステップ２２）ことを特徴とする。

【００１８】

請求項５記載の発明によれば、照合キーを通知するステップは、双方の利用者に異なる照合キーを通知することにより、確実に認証を行うことができる。

【００１９】

請求項６に記載された発明は、請求項１記載の認証処理方法において、更に、前記利用者間で予定した取引に関して第１の利用者に照合キーを通知するステップと、第１の利用者に通知された照合キーを第１の利用者より第２の利用者が受

け取った後に、第２の利用者から通知される前記第１の利用者の照合キーの照合を行うステップとを有することを特徴とする。

【００２０】

請求項６記載の発明によれば、更に、利用者間で予定した取引に関して第１の利用者に照合キーを通知するステップと、第１の利用者に通知された照合キーを第１の利用者より第２の利用者が受け取った後に、第２の利用者から通知される前記第１の利用者の照合キーの照合を行うステップとを有することにより、確実な認証を行うことができる。

【００２１】

請求項７に記載された発明は、請求項１ないし６いずれか一項記載の認証処理方法における照合結果に基づいて、決済処理（例えば、図２におけるステップ１９）を行うことを特徴とする。

【００２２】

請求項７記載の発明によれば、請求項１ないし６いずれか一項記載の認証方法における照合結果に基づいて、決済処理を行うことができる。

【００２３】

請求項８に記載された発明は、取引を行う利用者間の認証を行う認証処理システムにおいて、前記利用者間で予定した取引に関して第２の利用者に照合キーを通知する通知手段（例えば、図９における通知手段５５）と、第２の利用者に通知された照合キーを第２の利用者より第１の利用者が受け取った後に、第１の利用者から通知される前記第２の利用者の照合キーの照合を行う照合手段（例えば、図９における照合手段５７）とを有することを特徴とする。

【００２４】

請求項８記載の認証処理システムは、請求項１ないし６に記載された認証方法に適した認証処理システムを規定したものである。

【００２５】

請求項９に記載された発明は、取引を行う利用者間の認証に関する処理を行う利用者装置において、該取引に関して各利用者に異なる照合キーを通知する認証処理システムに、前記利用者間で予定した取引に関する情報を送信する第１の送

信手段（例えば、図１１における送信手段８０）と、前記認証システムからの該取引に関する照合キーを受信する第１の受信手段（例えば、図１１における受信手段８１）と、利用者間で前記照合キーを通知し合った後に、照合キーの照合を行う認証処理システムに、相手から通知された相手側の照合キーを、送信する第２の送信手段（例えば、図１１における送信手段８０）と、前記認証処理システムから照合結果を受信する第２の受信手段（例えば、図１１における受信手段８１）とを有することを特徴とする。

【００２６】

請求項９記載の利用者装置は、請求項１ないし６に記載された認証方法に適した利用者装置を規定したものである。

【００２７】

請求項１０に記載された発明は、取引を行う利用者間の認証に関する処理を行うためのプログラムを格納した記憶媒体であって、コンピュータを動作させて、

該取引に関して各利用者に異なる照合キーを通知する認証システムに、前記利用者間で予定した取引に関する情報を送信する第１の送信手段と、前記認証システムから該取引に関する照合キーを受信する第１の受信手段と、利用者間で前記照合キーを通知し合った後に、照合キーの照合を行う認証処理システムに、相手から通知された相手側の照合キーを、送信する第２の送信手段と、前記認証処理システムから照合結果を受信する第２の受信手段とを機能させるためのプログラムを格納したことを特徴とする。

【００２８】

請求項１０記載の取引を行う利用者間の認証に関する処理を行うためのプログラムを格納した記憶媒体は、請求項１ないし６に記載された認証方法に適した処理を行うためのプログラムを格納した記憶媒体を規定したものである。

【００２９】

【発明の実施の形態】

次に、本発明の実施の形態について図面と共に説明する。

【００３０】

本発明の認証及び決済システムの例を図１に示す。

【００３１】

図１は、利用者Ａ（第１の利用者、個人等）の端末１０$_1$～１０$_N$、利用者Ｂ（第２の利用者、店舗等）の端末２０$_1$～２０$_M$、インターネット等の通信ネットワーク３０、アプリケーション・サービス・プロバイダ４０から構成されている。また、プロバイダ４０は、認証・決済システム４１、利用者Ａデータベース４２及び利用者Ｂデータベース４３を有している。

【００３２】

利用者Ａは、サービスの提供を受ける又は物を購入する本システムの利用者である。また、利用者Ｂは、利用者Ａと取引を行う者で、サービスを提供する又は物を販売する本システムの利用者である。

【００３３】

利用者Ａデータベース４２には、利用者ＡのＩＤ番号、パスワード、決済情報及び商品を購入する資格の有無等の情報が格納され、利用者Ｂデータベース４３には、利用者ＢのＩＤ番号、パスワード、決済情報及び商品を販売する資格に関する有無等の情報が格納されている。

【００３４】

認証・決済システム４１は、後述するように、テンポラリな情報で、利用者Ａ

また、認証・決済システム４１は、利用者Ａデータベース４２に格納されている利用者ＡのＩＤ番号、パスワード、決済情報及び商品を購入する資格の有無等の情報及び利用者Ｂデータベース４３に格納されている利用者ＢのＩＤ番号、パスワード、決済情報及び商品を販売する資格に関する有無等の情報に基づいて、利用者Ａと利用者Ｂが、本サービスを受ける資格を有するか否かの資格チェック又はこれから行われる個別取引を行う資格を有するか否かの資格チェックを行う。

【００３５】

また、利用者Ａの端末１０$_1$～１０$_N$及び利用者Ｂの端末２０$_1$～２０$_M$は、固定端末でも携帯端末でもよい。ブラウザを搭載し、通信ネットワーク３０を介して、アプリケーション・サービス・プロバイダ４０に接続し、プロバイダ４０が提供するウエブページを閲覧することができる。

【００３６】

図２を参照して、訪問販売の認証・決済を説明する。

【００３７】

訪問販売員（利用者Ｂ）が玄関先に訪れた際に、自宅にいる人（利用者Ａ）の疑問である「この販売員と扱う商品の金額は妥当か」とか、訪問販売員の疑問である「この人は決済能力があるか」等を、携帯端末等を用いて解決できる。

【００３８】

つまり、以下に示す手順で認証を行い、それぞれが問題が無いことを確認した上で、商品を手渡すなどして取引を行う。

【００３９】

このシステムを利用する利用者Ａと利用者Ｂとが、アプリケーション・サービス・プロバイダ４０に加入していることが前提であり、利用者Ａと利用者Ｂとが、個々に、プロバイダに登録する（Ｓ１０）。

【００４０】

次いで、利用者Ｂが利用者Ａ宅を訪れ、利用者Ａの玄関で対面したとき、個々に、端末（携帯端末等）を用いて、プロバイダ４０に接続する。そのとき、利用者Ａと利用者Ｂとは、個々に、ＩＤ番号とパスワードを入力して、プロバイダから、本サービスが利用可能であることが認証される（Ｓ１１）。

【００４１】

次いで、利用者Ａと利用者Ｂとが、それぞれ、取引可能か否かの取引資格の確認を行う（Ｓ１２）。例えば、利用者Ａは、商品の購入をする資格を有しているか否かであり、利用者Ｂは、商品の販売をする資格を有しているか否かである。

【００４２】

プロバイダ４０は、利用者Ａデータベース４２及び利用者Ｂデータベース４３を参照して認証を行う。従って、商品の購入をする資格を有していない利用者Ａは、この時点で以降の処理ができなくなる。また、商品の販売をする資格を有していない利用者Ｂは、この時点で以降の処理ができなくなる。

【００４３】

これにより、例えば、購買資力ない利用者Ａ、販売資格のない利用者Ｂを排除

できるので、安心して、取引ができる。

【００４４】

利用者Ａが商品の購入をする資格を有しており、利用者Ｂが、商品の販売をする資格を有している場合は、取引キーの選定を行う（Ｓ１３）。

【００４５】

図３に取引ページの画面の例を示す。図３の取引ページの画面では、取引キー１～取引キーＮと、その取引キーに関連する利用者Ａのボタン50_1～50_N及び利用者Ｂのボタン51_1～51_Nを有している。

【００４６】

利用者Ａと利用者Ｂは、同じ、取引ページの画面を閲覧する。取引ページの画面には、利用可能な取引キーが示されている。

【００４７】

利用者Ａと利用者Ｂは、互いに、どの取引キーを利用するかを決めて（Ｓ１３）、個々に、ボタンをクリックする。例えば、取引キー２を利用するのであれば、利用者Ａはボタン50_2をクリックし、利用者Ｂはボタン51_2をクリックする。

【００４８】

ボタン50_2とボタン51_2が押されると、プロバイダ４０から、利用者Ａと利用者Ｂに対して、それぞれ、照合キーが通知され、それぞれ、利用者Ａと利用者Ｂの画面に表示される（Ｓ１４）。

【００４９】

次いで、利用者Ａと利用者Ｂとは、プロバイダ４０から通知された照合キーを互いに、口頭等で通知する（Ｓ１５）。

【００５０】

次いで、利用者Ａと利用者Ｂは、個々に、共通の取引番号（ここでは、取引キー２に対応した番号）に対して、相手から通知された、照合キーを入力する（Ｓ１６）。

【００５１】

前記プロバイダ４０は、共通の取引番号と利用者Ａと利用者Ｂからの二つの照

合キーが、それぞれ、前記個別取引に関して、前記プロバイダ４０が通知した照合キーであるか否かを判定してキーの照合を行う（Ｓ１７）。

【００５２】

プロバイダ４０は、判定した結果を利用者Ａと利用者Ｂに通知する（Ｓ１８）。

【００５３】

照合がＯＫであれば、相手に問題が無いことが確認されたので、商品を手渡すなどして、取引を完了する。

【００５４】

次いで、プロバイダ４０の決済機能等を利用して決済を行う（Ｓ１９）。

【００５５】

なお、必要であれば、利用者Ａと利用者Ｂが、プロバイダ４０から通知された照合キーを互いに通知するとき、決済に必要な金額等を通知・確認してもよい。

【００５６】

また、利用者Ｂは、個人であっても、企業であってもよい。

【００５７】

照合の方法（上記図２におけるＳ１４～Ｓ１８）について、図４を用いて説明する。

【００５８】

上記図３において、取引キー２に関して、利用者Ａがボタン５０$_2$をクリックし、利用者Ｂが、ボタン５１$_2$をクリックすると、利用者Ａに個別キー（照合キー）（Ａ）が通知され、利用者Ｂに個別キー（照合キー）（Ｂ）が通知される（Ｓ２１、Ｓ２２）。

【００５９】

個別キー（Ａ）と個別キー（Ｂ）は、それぞれ異なるキーであり、取引キー２に関連する情報である。個別キー（Ａ）と個別キー（Ｂ）とは、取引キー２の割り符に相当し、個別キー（Ａ）と個別キー（Ｂ）とが合わされば、取引キー２がＯＫとなるイメージである。

【００６０】

取引キー２は、利用者Ａと利用者Ｂとで共有している。しかしながら、個別キー（Ａ）は、利用者Ａのみが知っている情報であり、個別キー（Ｂ）は、利用者Ｂのみが知っている情報である。

【００６１】

次いで、利用者Ａと利用者Ｂとは、それぞれの個別キー（Ａ）と個別キー（Ｂ）を交換する（Ｓ２３）。

【００６２】

次いで、利用者Ａと利用者Ｂは、プロバイダが提供する画面において、取引キー２に関して、相手から通知された、それぞれ入力する（Ｓ２５、Ｓ２６）。

【００６３】

個別キーの入力は、例えば、Ｓ２６に示すように、プロバイダ４０が提供する、同じ画面を閲覧し、利用者Ａと利用者Ｂは、それぞれ、画面の（Ａ）及び（Ｂ）に、相手から通知された個別キーを入力する。

【００６４】

なお、Ｓ２６の「××××××」には、個別キー自体は、表示されない。

【００６５】

プロバイダ４０は、利用者Ａの個別キー（Ａ）と取引相手から取得した個別キー（Ｂ）とが、取引キー２の割り符であるか否かを判定し、その結果を、利用者Ａに通知し（Ｓ２７）、利用者Ｂの個別キー（Ｂ）と取引相手から取得した個別キー（Ａ）とが、取引キー２の割り符であるか否かを判定し、その結果を、利用者Ｂに通知する（Ｓ２８）。

【００６６】

符合すれば、目の前にいる人は、プロバイダ４０が認証した、売買の資格を有する人であることが確認できたので、安心して取引を行うことができる。

【００６７】

本発明は、レストランでの活用も可能である。以下に、レストランの例を実施例として、図５～図７を用いて説明する。

【００６８】

このシステムを利用するレストランの利用者とレストランとが、同じアプリケ

ーション・サービス・プロバイダに加入していることが前提であり、レストランの利用者とレストランとが、個々に、プロバイダに登録する。

図５（Ａ）は、レストランの利用者が、プロバイダに登録し（Ｓ３０）、個別ＩＤとパスワードを払い出す（Ｓ３１）フローの例である。

図５（Ｂ）は、レストランが、プロバイダに登録し（Ｓ３２）、個別ＩＤとパスワードを払い出す（Ｓ３３）フローの例である。

図６は、取引を開始して、レストランの利用者が、レストランに行くまでの処理フローの例を示す。

【００６９】

レストランの利用者は、端末（パソコン、携帯端末等）から、プロバイダに接続し、ＩＤ／パスワードを入力してログインを行う（Ｓ４０）。次いで、レストランの利用者は、取引種別／認証範囲を指定する（Ｓ４１）。具体的には、レストランの利用者が利用しようとする店の特定とサービスの提供受けたい又は物を購入したいとの申し出を行い、さらに、必要に応じて、レストランの利用者が受けたい保証の範囲を指定する。

【００７０】

このとき、レストランの利用者は、必要に応じて、取引の条件（例えば、個室であるか否か又はランク等）を示すようにしてもよい。

【００７１】

取引キーを選択して、プロバイダから個別キー（Ａ）を取得する（Ｓ４２）。

【００７２】

その後、プロバイダは、指定されたレストランに、取引依頼（利用予約）があったことを、取引キーと共に、電子メール等で通知する（Ｓ４３）。

【００７３】

レストランでは、取引依頼（利用予約）があったことを受けて（Ｓ４４）、プロバイダに接続し、ＩＤ／パスワードを入力してログインを行う（Ｓ４５）。次いで、通知された取引キーを選択又は入力して、プロバイダから個別キー（Ｂ）を取得する（Ｓ４６）。

【００７４】

図７は、レストランの受付カウンターでの処理フローの例を示す。

【００７５】

レストランの利用者は、受付カウンターにおいて、口頭で、取引キーと個別キー（Ａ）をレストランの受付の人に通知する（Ｓ５０）。

【００７６】

なお、取引キー（Ａ）と個別キーのレストランへの通知は、電子メールで行われても良いし、レストランの利用者に代わって、プロバイダが行ってもよい。

【００７７】

レストランの受付の人は、口頭等で、取引キーと個別キー（Ｂ）をレストランの利用者に通知する（Ｓ５１）。

【００７８】

その後、レストランとレストランの利用者は、別々に、プロバイダに接続し、ＩＤ／パスワードを入力してログインを行う（Ｓ５２、Ｓ５４）。

【００７９】

レストランの利用者は、プロバイダが提供する画面で、取引キーと個別キー（Ｂ）と金額を入力する（Ｓ５３）。同じく、レストランは、プロバイダが提供する画面で、取引キーと個別キー（Ａ）と金額を入力する（Ｓ５４）。

【００８０】

プロバイダでは、取引キーに対して、それぞれの個別キーが照合するか否かを判定し、照合した結果を、金額と共に、レストランとレストランの利用者に通知する（Ｓ５６）。

【００８１】

レストランとレストランの利用者の端末には、照合された結果が表示される（Ｓ５７、Ｓ５８）。

【００８２】

この結果、予約したレストランの利用者は、所望した条件のサービスを受けることができる。

【００８３】

なお、金額の入力欄を設け無くてもよい。また、金額の入力欄に記入しなくて

も、認証を行うようにしてもよい。

【００８４】

上述の通り、プロバイダ４０は、共通の取引キーと利用者Ａと利用者Ｂからの二つの識別キー（個別キー（Ａ）と個別キー（Ｂ））が、符号するか否かで、照合している。

【００８５】

これには、二つのタイプがある。

【００８６】

一つは、図８（Ａ）に示したように、共通の取引キーに対して、プロバイダが、個別キー（Ａ）と個別キー（Ｂ）を払い出す場合で、上述の例は、図８（Ａ）の例に相当する。

【００８７】

一方、図８（Ｂ）は、個別キー（Ａ）と個別キー（Ｂ）とに、それぞれ、ユニークな情報を設定し、共通の取引キーとしては、個別キー（Ａ）と個別キー（Ｂ）とから生成されるキーを用いる。

【００８８】

ユニークな情報として、認証に使用する個別ＩＤを用いることも可能である。しかしながら、セキュリティ上のことを考慮して、認証に使用する個別ＩＤ自体でなく、例えば、ログオン時に、払いだされたテンポラリな個別ＩＤを使用するようにしてもよい。

【００８９】

共通の取引キー自体は、取引を識別できれば良いので必ずしも、秘密にする必要も無いが、他の取引キーと区別するために、独自の取引キーを生成することが好ましい。

【００９０】

例えば、共通の取引キーとして、単に、個別キー（Ａ）と個別キー（Ｂ）とを並べたものでも良いし、個別キー（Ａ）と個別キー（Ｂ）を基に、何らかの論理演算処理を施したものでもよい。

【００９１】

例えば、個別キー（Ａ）が「１２３４」であり、個別キー（Ｂ）が「５６７８」の場合、共通の取引キーとして、単に並べた、「１２３４５６７８」としてもよい。また、共通の取引キーとして、両者を掛け算した、「７００６６５２」としてもよい。また、個別キー（Ａ）と個別キー（Ｂ）と２進数の論理演算でもよい。

【００９２】

図８（Ｂ）では、プロバイダは、個別キーの払い出しの処理が不要となる。

【００９３】

なお、本発明は、ホテル予約システムでの活用も可能である。

【００９４】

例えば、プロバイダに加入しているホテルを予約する場合、インターネット接続可能な携帯端末（電話）を通じて、事前に予約し、照合キーＡ（予約番号）を取得する。予約先のホテルでは、予約者の予約を確認し、照合キーＢ（確認番号）を予約者に通知する。

【００９５】

予約者は、確認番号を入力することでホテルに対する照合を完了する。一方、ホテルは、利用時に予約者から予約番号を確認し利用者本人を確認するとともに、決済を確認する。

【００９６】

さらに、本発明は、遊園地・映画館等での入場予約システムとして活用できる。

【００９７】

例えば、プロバイダに加盟している遊園地などの施設を利用する場合は、事前に予約番号を取得し、内部的に情報照合を終えておくことで、予約先の施設に入園する際に予約番号を施設側パソコンなどから入力することで入場を可能とする。

と利用者Ｂ間の認証を行い、安全で利便性の高い認証・決済手段を提供する。

【００９８】

図９に認証・決済システム４１における主要な機能ブロックの例を示す。

【００９９】

決済手段５４は、認証と取引が行われた場合、当該取引に関して決済を行う。

【０１００】

通知手段５５は、取引に関して、双方の利用者に異なる照合キーを通知し、照合の結果、取引に係る通知等を行う。

【０１０１】

受取手段５６は、取引に関して各利用者に通知した照合キーであって、利用者間で交換した照合キー等を受け取る。

【０１０２】

照合手段５７は、一方の利用者に通知された照合キーを他方の利用者が受け取った後に、他方の利用者から通知される一方の利用者の照合キーに係る照合、他方の利用者に通知された照合キーを一方の利用者が受け取った後に、一方の利用者から通知される他方の利用者の照合キーに係る照合等を行う。

【０１０３】

資格チェック手段５８は、本システムを利用する資格が有るか否か、取引を行う資格が有るか否かのチェック等を行う。

【０１０４】

図１０に、サーバ４０のハードウェア構成の例を示す。

【０１０５】

図１０では、キーボード、ポインティングデバイス等の入力装置６１、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ　：中央処理装置）６２、ＲＯＭ（Ｒｅａｄ　ｏｎｌｙ　ｍｅｍｏｒｙ）６３、ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　ｍｅｍｏｒｙ）６４、通信ネットワーク２０とインタフェースをとる通信ＩＦ（インタフェース）６５、内部バス６６、外付けのＨＤＤ（Ｈａｒｄ　Ｄｉｓｋ　Ｄｒｉｖｅ）、プリンタ、スキャナとインタフェースを取るＩＦ（インタフェース）６７、ＨＤＤ６８、ＦＤ（Ｆｌｏｐｐｙ　Ｄｉｓｋ）の書込み及び読出しを行うＦＤＤ（Ｆｌｏｐｐｙ　Ｄｉｓｋ　Ｄｒｉｖｅ）６９、ＣＤ－ＲＯＭの読み込みを行うＣＤ－ＲＯＭドライブユニット７０，ディスプレイ７４の表示コントローラ７１から構成されている。

【０１０６】

ハードウェア自体の機能は、周知であるので説明を省略する。

【０１０７】

本発明の認証処理を行うためのプログラムを記録した記憶媒体を作成し、この記録媒体から、本発明の認証処理を行うためのプログラムを読み出して、ＣＰＵ６２に実行させて、認証処理を行うことができる。

【０１０８】

なお、本発明の認証処理を行うためのプログラムを記録した記憶媒体は、フロッピディスク、ハードディスク、光ディスク（ＣＤ－ＲＯＭ、ＣＤ－Ｒ、ＣＤ－Ｒ／Ｗ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭなど）、光磁気ディスク、メモリカードなどであってもよい。

【０１０９】

図１１に利用者端末（Ａ、Ｂ）における主要な機能ブロックの例を示す。

【０１１０】

図１１では、送信手段８０、受信手段８１、入力手段８２及び出力手段８３から構成されている。

【０１１１】

送信手段８０は、利用者間で予定した取引に関する情報をサーバに送信し、更に、利用者間で照合キーを交換して得た相手側の照合キー等を送信する。

【０１１２】

受信手段８１は、サーバからの取引に関する照合キーを受信し、更に、照合結果等を受信する。

【０１１３】

入力手段８２は、認証・決済処理に必要な事項を入力する。例えば、ＩＤ、パスワード、照合キー等の入力を行う。

【０１１４】

出力手段８３は、認証・決済処理において、利用者端末に送られた情報を表示する。

【０１１５】

以上の通り、本発明の実施の形態又は実施例によれば、カード又は現金を所持する必要がなくなる。

【０１１６】

ところで、現実社会におけるカード又は現金の支払いにおいては、常にカード又は現金を所持していなければならず、紛失、盗難の可能性が高い。また、カード又は現金を所持していない場合は、買い物又はサービスを受けられないなど利便性が悪い。また、カード利用時には、カード番号漏洩など安全性（セキュリティ）、信頼性においても少なからず問題が残っている。

【０１１７】

本発明では、カード又は現金を所持する必要がないことにより、上記問題が無くなる。

【０１１８】

上述の如く、本発明によれば、テンポラリな情報で認証を可能とし、安全で利便性の高い認証・決済手段を提供することができる。

【０１１９】

また、プロバイダの加入情報をベースに認証し合うことにより、カード又は現金を所持することなく、決済処理が可能となり、カード又は現金を所持上の問題は解消される。

【０１２０】

また、カード又は現金を所持しなくとも、リアルタイムの取引が可能となり、安全に各種対面販売取引を行うことが可能となる。

【０１２１】

次に、発明の態様を付記として示す。

（付記１）取引を行う利用者間の認証に関する処理を行う認証処理システムにおける認証処理方法において、

前記利用者間で予定した取引に関して第２の利用者に照合キーを通知するステップと、

第２の利用者に通知された照合キーを第２の利用者より第１の利用者が受け取った後に、第１の利用者から通知される前記第２の利用者の照合キーの照合を行

うステップとを有することを特徴とする認証処理方法。（１）

（付記２）付記１記載の認証処理方法において、

前記認証処理システムは、照合キーを通知するステップに先だって、利用者の個人認証を行うことを特徴とする認証処理方法。（２）

（付記３）付記１記載の認証処理方法において、

前記取引が予め設定された利用可能金額内であるか否かの判定を行うことを特徴とする認証処理方法。（３）

（付記４）付記１記載の認証処理方法において、

前記取引が予め設定された取引条件に適合するか否かの判定を行うことを特徴とする認証処理方法。（４）

（付記５）付記１記載の認証処理方法において、

前記照合キーを通知するステップは、双方の利用者に異なる照合キーを通知することを特徴とする認証処理方法。（５）

（付記６）付記１記載の認証処理方法において、

前記利用者は、前記認証処理システムが提供する同じ画面を閲覧し、それぞれの端末で表示されている画面上で、認証に必要な情報を選択又は入力することを特徴とする認証処理方法。

【０１２２】

なお、付記６に記載された発明によれば、利用者は、同じウエブページを閲覧しながら、認証を行うことができるので、確実にしかも簡便に行うことができる。

（付記７）付記１記載の認証処理方法において、更に、

前記利用者間で予定した取引に関して第１の利用者に照合キーを通知するステップと、

第１の利用者に通知された照合キーを第１の利用者より第２の利用者が受け取った後に、第２の利用者から通知される前記第１の利用者の照合キーの照合を行うステップとを有することを特徴とする認証処理方法。（６）

（付記８）付記１記載の認証処理方法において、

前記利用者の照合キーは、前記利用者を特定するユニークな情報であることを

特徴とする認証処理方法。

【０１２３】

付記８に記載された発明によれば、利用者の照合キーとして、利用者を特定するユニークな情報を用いることにより、プロバイダ等の処理負担を減少させることができる。

（付記９）付記１ないし８いずれか一項記載の認証処理方法における照合結果に基づいて、決済処理を行うことを特徴とする決済方法。（７）

（付記１０）　取引を行う利用者間の認証を行う認証処理システムにおいて、

前記利用者間で予定した取引に関して第２の利用者に照合キーを通知する通知手段と、

第２の利用者に通知された照合キーを第２の利用者より第１の利用者が受け取った後に、第１の利用者から通知される前記第２の利用者の照合キーの照合を行う照合手段とを有することを特徴とする認証処理システム。（８）

（付記１１）　取引を行う利用者間の認証に関する処理を行う利用者装置において、

該取引に関して各利用者に異なる照合キーを通知する認証処理システムに、前記利用者間で予定した取引に関する情報を送信する第１の送信手段と、

前記認証システムからの該取引に関する照合キーを受信する第１の受信手段と、

利用者間で前記照合キーを通知し合った後に、照合キーの照合を行う認証処理システムに、相手から通知された相手側の照合キーを、送信する第２の送信手段と、

前記認証処理システムから照合結果を受信する第２の受信手段とを有することを特徴とする利用者装置。（９）

（付記１２）　取引を行う利用者間の認証に関する処理を行うためのプログラムを格納した記憶媒体であって、

コンピュータを動作させて、

該取引に関して各利用者に異なる照合キーを通知する認証システムに、前記利用者間で予定した取引に関する情報を送信する第１の送信手段と、

前記認証システムから該取引に関する照合キーを受信する第１の受信手段と、

利用者間で前記照合キーを通知し合った後に、照合キーの照合を行う認証処理システムに、相手から通知された相手側の照合キーを、送信する第２の送信手段と、

前記認証処理システムから照合結果を受信する第２の受信手段とを機能させるためのプログラムを格納したことを特徴とする記憶媒体。（１０）

【発明の効果】

上述の如く本発明によれば、次に述べる種々の効果を奏することができる。請求項１記載の発明によれば、利用者間で予定した取引に関して第２の利用者に照合キーを通知し、更に、第２の利用者に通知された照合キーを第２の利用者より第１の利用者が受け取った後に、第１の利用者から通知される前記第２の利用者の照合キーの照合を行うことにより、テンポラリな情報で認証が可能となり、安全で利便性の高い認証を行うことができる。

【０１２４】

請求項２記載の発明によれば、認証処理システムは、照合キーを通知するステップに先だって、利用者の個人認証を行うことにより、取引当事者は、相手の資格・当事者能力について心配することなく、安心して取引を行うことができる。

【０１２５】

請求項３記載の発明によれば、取引が予め設定された利用可能金額内であるか否かの判定を行うことにより、取引当事者は、金額の心配をすることなく、安心して取引を行うことができる。

【０１２６】

請求項４記載の発明によれば、取引が予め設定された取引条件に適合するか否かの判定を行うことにより、取引当事者は、取引条件に関して心配をすることなく、安心して取引を行うことができる。

【０１２７】

請求項５記載の発明によれば、照合キーを通知するステップは、双方の利用者に異なる照合キーを通知することにより、確実に認証を行うことができる。

【０１２８】

請求項６記載の発明によれば、更に、利用者間で予定した取引に関して第１の利用者に照合キーを通知するステップと、第１の利用者に通知された照合キーを第１の利用者より第２の利用者が受け取った後に、第２の利用者から通知される前記第１の利用者の照合キーの照合を行うステップとを有することにより、確実な認証を行うことができる。

【０１２９】

請求項７記載の発明によれば、請求項１ないし６いずれか一項記載の認証方法における照合結果に基づいて、決済処理を行うことができる。

【０１３０】

請求項８記載の発明によれば、請求項１ないし６に記載された認証方法に適した認証処理システムを提供することができる。

【０１３１】

請求項９記載の発明によれば、請求項１ないし６に記載された認証方法に適した利用者装置を提供することができる。

【０１３２】

請求項１０記載の発明によれば、請求項１ないし６に記載された認証方法に適した処理を行うためのプログラムを格納した記憶媒体を提供することができる。

【図面の簡単な説明】

【図１】

本発明の認証及び決済システムの例を説明するための図である。

【図２】

認証及び決済の処理フローの例である。

【図３】

取引ページ画面例である。

【図４】

取引の照合を説明するための処理フローの例である。

【図５】

前処理の処理フローの例である。

【図６】

取引を開始して、レストランの利用者が、レストランに行くまでの処理フローの例である。

【図７】

レストランの受付カウンターでの処理フローの例である。

【図８】

取引の照合を説明するための図である。

【図９】

認証・決済システムにおける主要な機能ブロックの例を説明するための図である。

【図１０】

プロバイダのハードウェア構成の例を説明するための図である。

【図１１】

利用者端末（Ａ、Ｂ）における主要な機能ブロックの例を説明するための図である。

【符号の説明】

10_1～10_N　利用者Ａ（サービスの提供を受ける又は物を購入する第１の利用者）端末

20_1～20_M　利用者Ｂ（サービスを提供する又は物を販売する第２の利用者）端末

３０　通信ネットワーク

４０　アプリケーション・サービス・プロバイダ

４１　認証・決済システム

４２　利用者Ａのデータベース

４３　利用者Ｂのデータベース

５４　決済手段

５５　通知手段

５６　受取手段

５７　照合手段

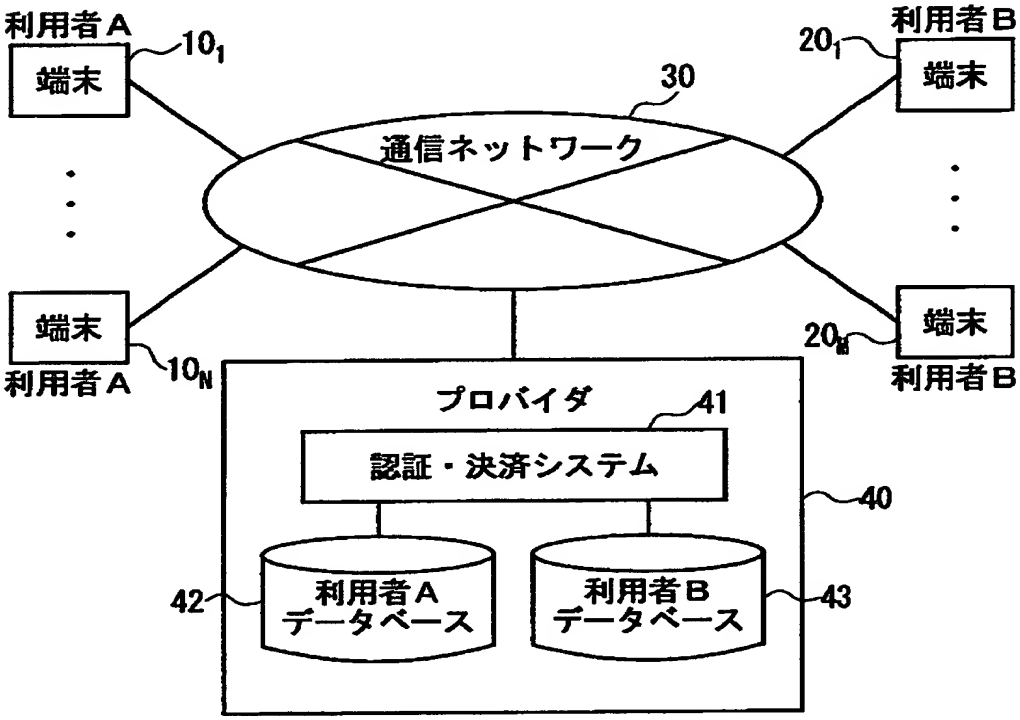
５８　資格チェック手段

６１　入力装置
６２　ＣＰＵ
６３　ＲＯＭ
６４　ＲＡＭ
６５　通信ＩＦ
６７　ＩＦ
６８　ＨＤＤ
６９　ＦＤＤ
７０　ＣＤ－ＲＯＭドライブユニット
７１　表示コントローラ
７２　ＦＤ
７３　ＣＤ－ＲＯＭ
７４　ディスプレイ
８０　送信手段
８１　受信手段
８２　入力手段
８３　出力手段

【書類名】　図面

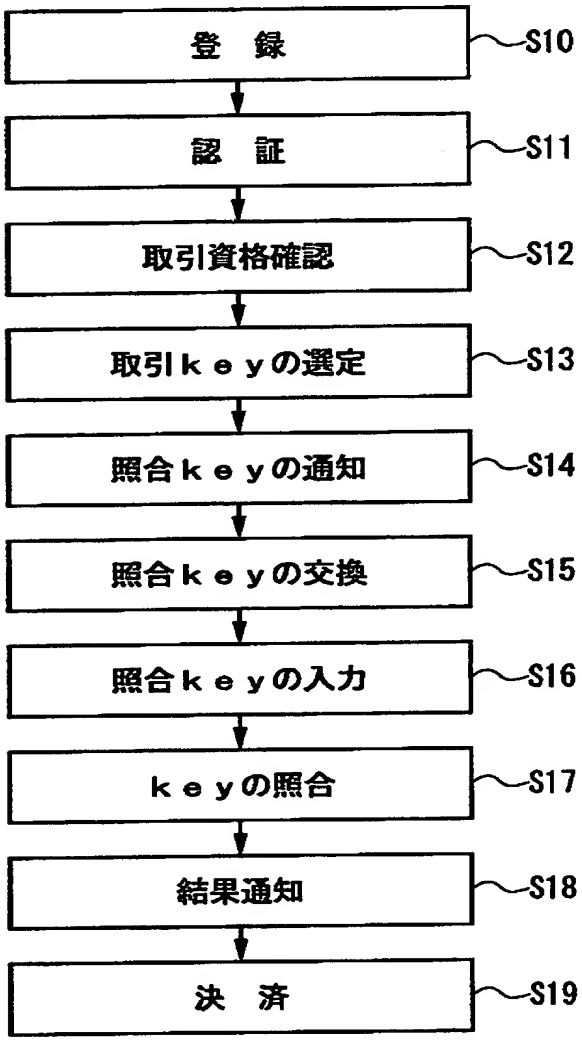
【図１】

本発明の認証及び決済システムの例を説明するための図

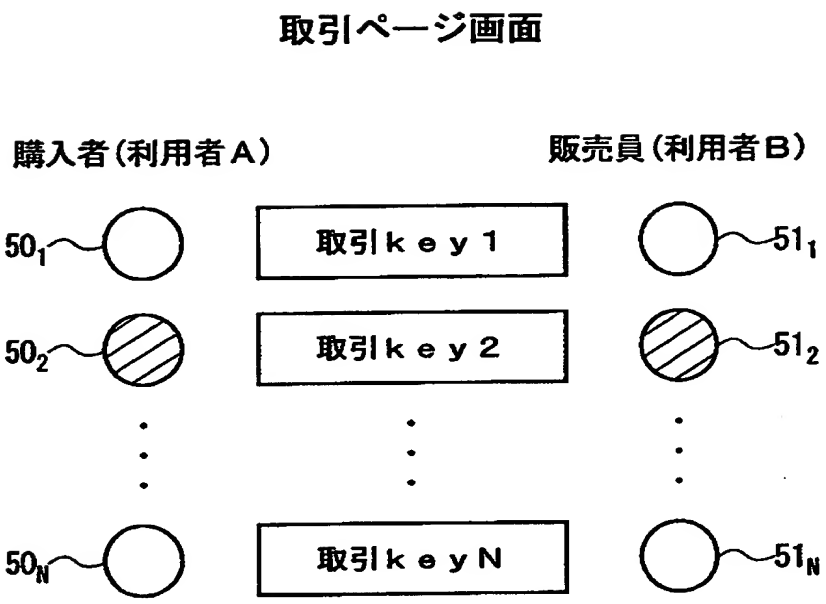


【図２】

相互認証及び決済の処理フローの例

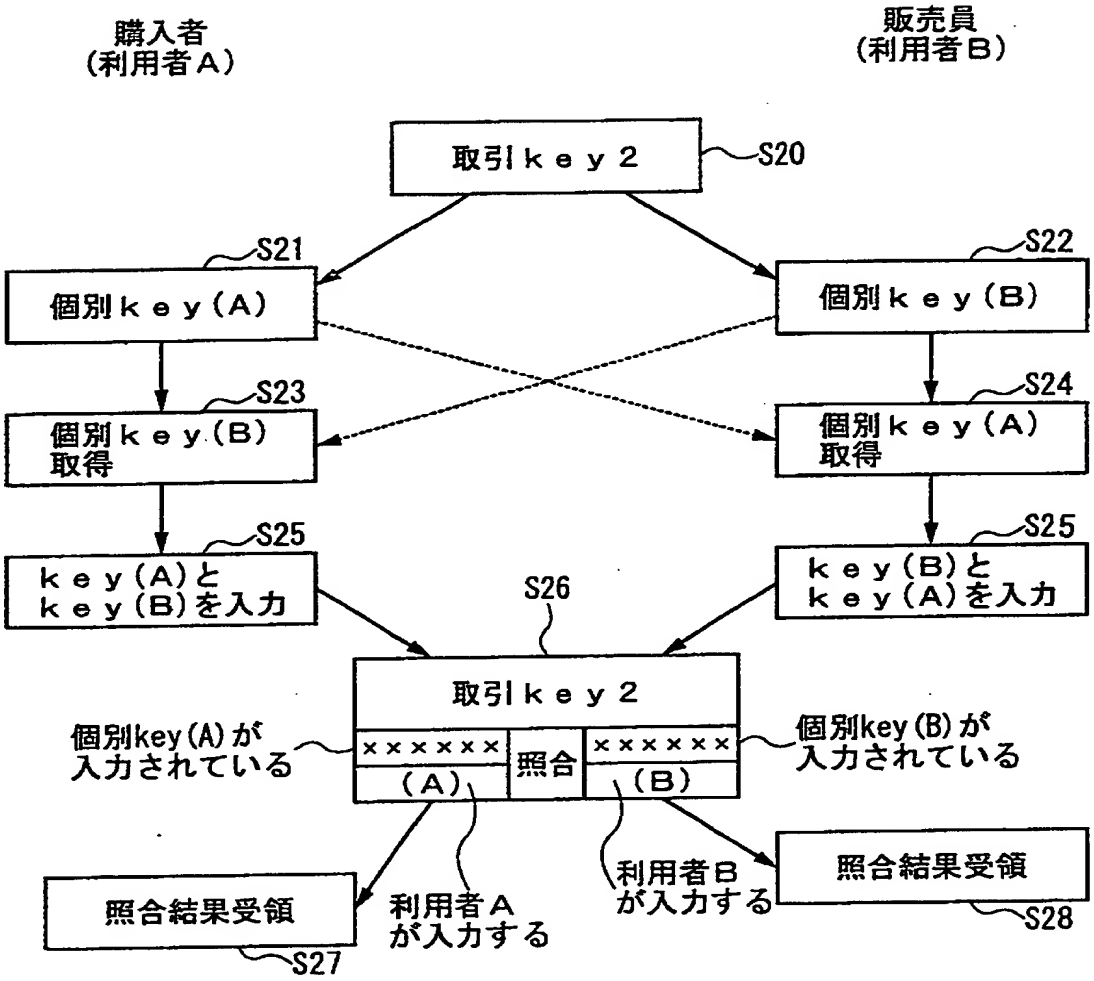


【図３】


取引ページ画面
購入者（利用者Ａ）
販売員（利用者Ｂ）
50_1
50_2
50_N
取引ｋｅｙ１
取引ｋｅｙ２
取引ｋｅｙＮ
51_1
51_2
51_N

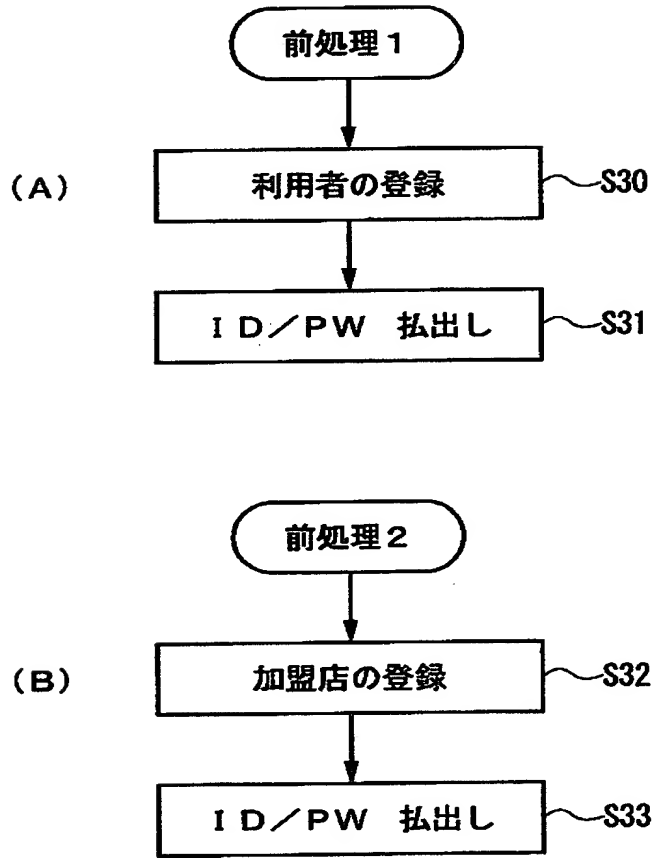
【図４】

取引の照合を説明するための処理フローの例



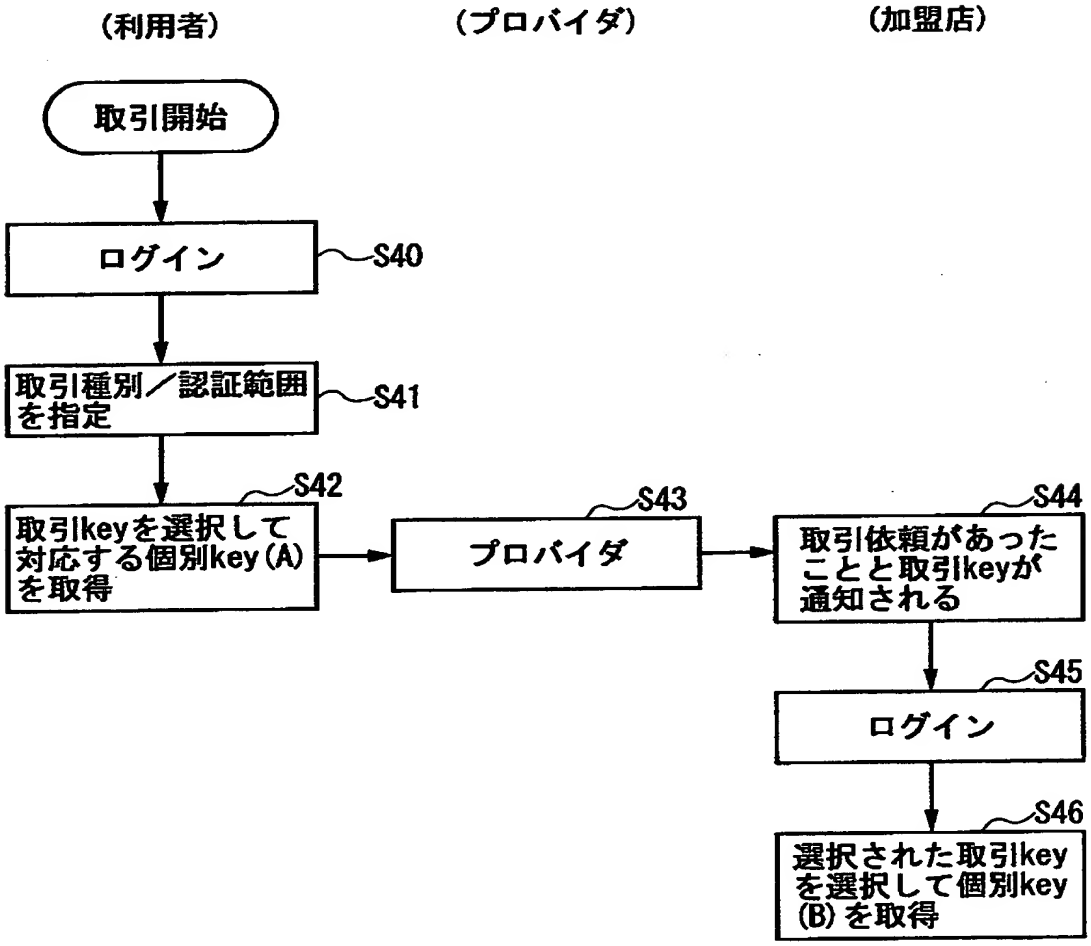
【図５】

前処理の処理フローの例



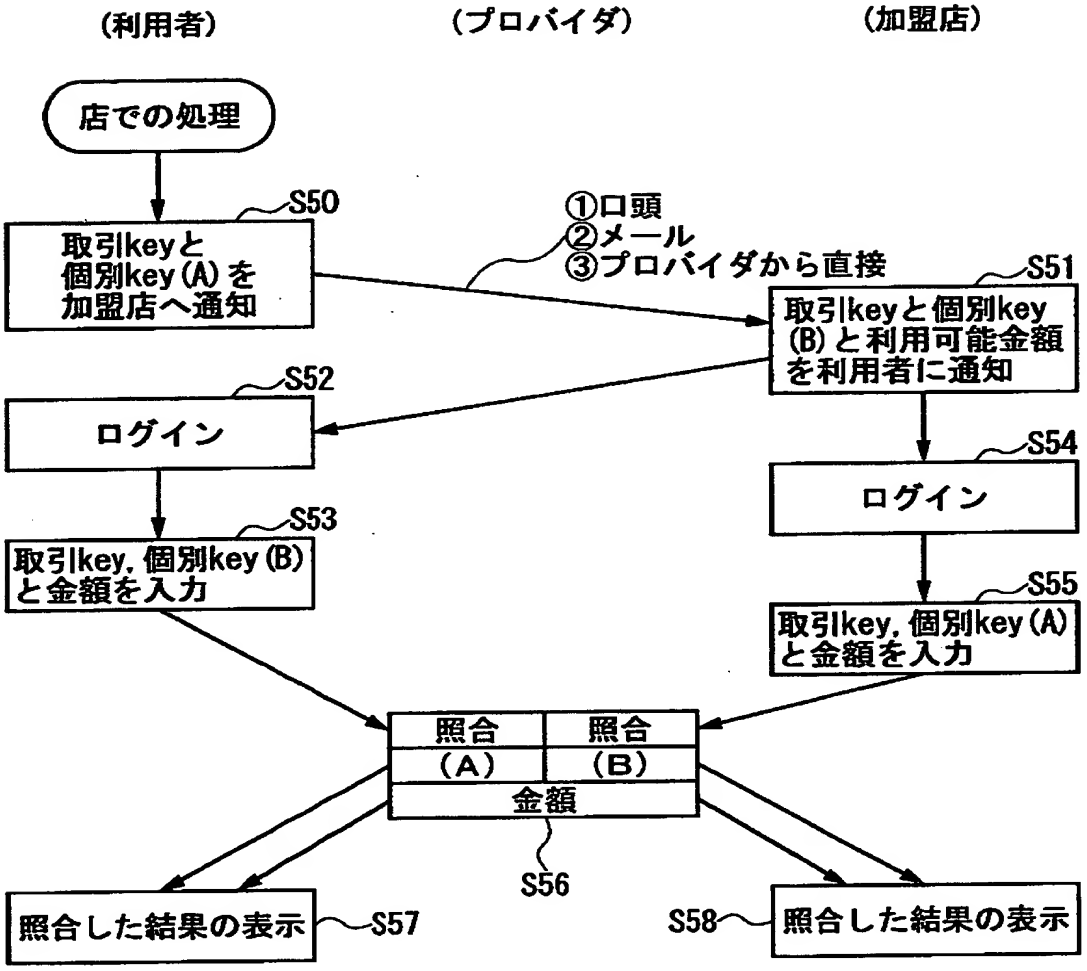
【図６】

取引を開始して、レストランの利用者がレストランに行くまでの処理フローの例



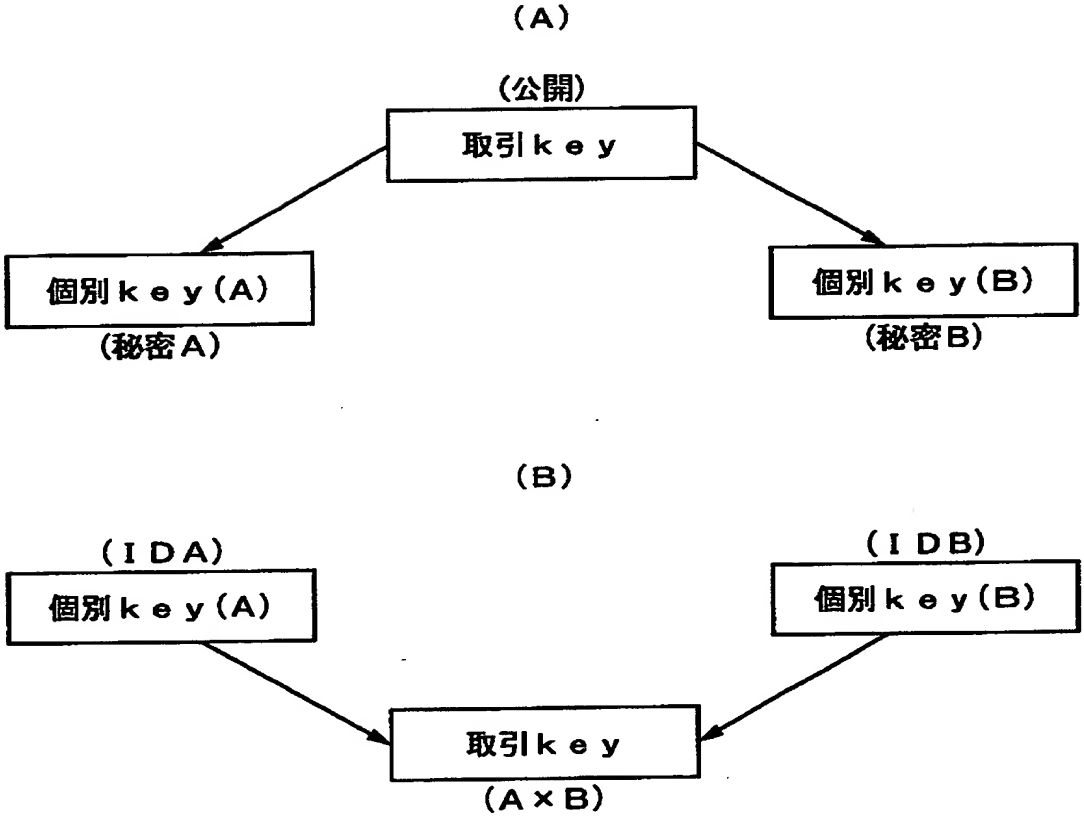
【図７】

レストランの受付カウンターでの処理フローの例



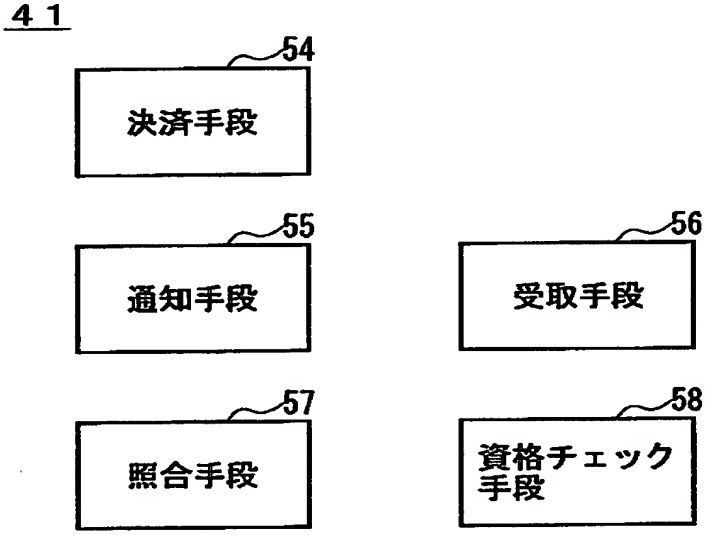
【図８】

取引の照合を説明するための図



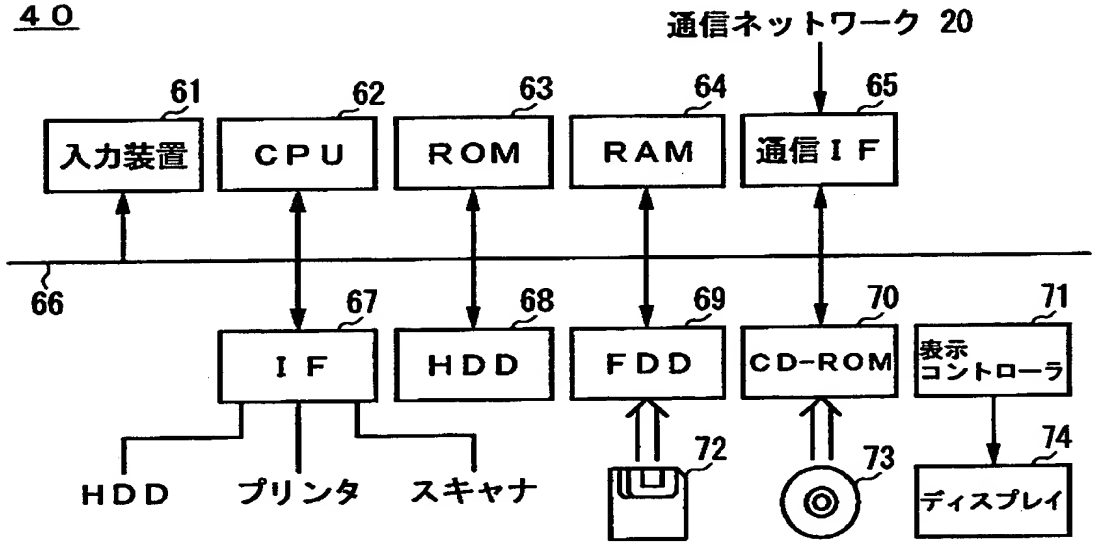
【図９】

認証・決済システムにおける主要な機能ブロックの例を説明するための図



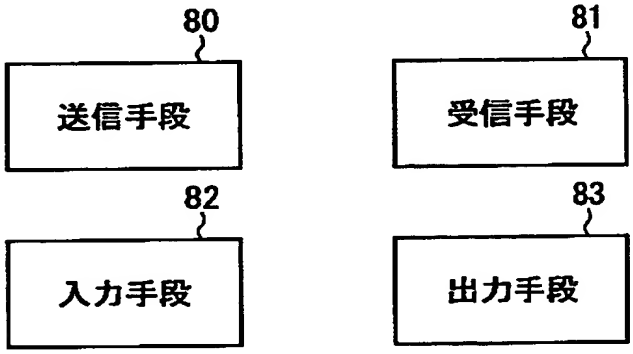
【図１０】

プロバイダのハードウェア構成の例を説明するための図



【図１１】

利用者端末(A, B)における
主要な機能ブロックの例を説明するための図



出証特２０００－３１０１１８１

【書類名】　　要約書

【要約】

【課題】　テンポラリな情報で認証を可能とし、安全で利便性の高い認証・決済手段を提供することを目的とする。

【解決手段】初対面時に、利用者Ｂと、利用者Ａとで認証を行う例である。予め、利用者Ａと利用者Ｂは、プロバイダに登録する（Ｓ１０）。対面したとき、個々の端末を用いて、本サービスが利用可能であること認証し（Ｓ１１）、更に、取引資格の確認を行う（Ｓ１２）。次いで、利用者Ａと利用者Ｂは、同一の取引キーの選定を行い（Ｓ１３）、プロバイダから、それぞれ、異なる照合キーを受ける（Ｓ１４）。利用者Ａと利用者Ｂは、その照合キーを交換し（Ｓ１５）、相手から通知された照合キーを、プロバイダが提供する画面上で入力する（Ｓ１６）。プロバイダは、照合キーの照合を行い（Ｓ１７）、その結果を、利用者Ａと利用者Ｂに通知する（Ｓ１８）。その後、必要に応じて、決済する（Ｓ１９）。

【選択図】　　図２

出　願　人　履　歴　情　報

識別番号　　〔０００００５２２３〕

１．変更年月日　　１９９６年　３月２６日
［変更理由］　住所変更
住　所　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　富士通株式会社